Supreme Court, U.S.
FILED
07-265 AUG 27 2007
OFFICE OF THE CLERK

No. ———

In The

Supreme Court of the United States

JAVIER PEREZ,

Petitioner,

vs.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The Fifth Circuit Court Of Appeals

PETITION FOR WRIT OF CERTIORARI

CHRISTOPHER M. PERRI
2906 N. Broadway, #3
Chicago, IL 60657
(773) 868-0360
Fax No. (512) 474-8252
Texas Bar Number:
24047769

JOSEPH A. TURNER
(*Counsel of Record*)
1504 West Ave.
Austin, TX 78701
(512) 474-4892
Fax No. (512) 474-8252
Texas Bar Number:
20322500

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

QUESTION PRESENTED FOR REVIEW

Does the fact that illegal activity emanates from an IP address establish probable cause to search the property of the registered owner of that IP address when multiple people use the same IP address?

PARTIES TO THE PROCEEDING

Petitioner, Javier Perez, was the sole defendant in the criminal proceedings below. The United States prosecuted the case.

TABLE OF CONTENTS

	Page
QUESTION PRESENTED FOR REVIEW	i
PARTIES TO THE PROCEEDING	ii
TABLE OF AUTHORITIES	v
PETITION FOR WRIT OF CERTIORARI	1
CITATION TO REPORTS OF OPINIONS ENTERED	1
JURISDICTIONAL STATEMENT	1
RELEVANT CONSTITUTIONAL PROVISION	1
STATEMENT OF THE CASE	2
REASONS FOR GRANTING THE WRIT	7
The Fifth Circuit has decided an important federal question in a way that conflicts with relevant decisions of this Court, as the Fifth Circuit has sanctioned a standard for the issuance of search warrants in cyber-crime cases that ignores the realities of Internet technology and falls below a rational conception of probable cause	7
A. The fact that illegal transmissions emanate from an IP address that is registered to a specific person does not establish probable cause to search the registrant's property unless there is evidence that the registrant is the sole user of that IP address	9
B. Once the executing officers discovered that multiple residents lived at Petitioner's residence, they should have discontinued the execution of the search warrant because there was no longer probable cause to search Petitioner's property	13

TABLE OF CONTENTS – Continued

Page

C. Upon receiving new information from the executing officers, a neutral magistrate would have concluded that there was no longer probable cause to search Perez's property 14

D. The Fifth Circuit has sanctioned a standard of probable cause in the realm of cyber-crime search warrants that violates basic notions of fairness, as innocent landlords and employers will be the subject of intrusive search warrants unless the Supreme Court acts 16

APPENDIX

Fifth Circuit Opinion ..... App. 1

District Court Order and Opinion ..... App. 18

Fifth Circuit's Order on Petition for Panel Rehearing ..... App. 31

Affidavit in Support of Search Warrant ..... App. 32

Excerpts from Transcript of Hearing on Motion to Suppress ..... App. 47

Excerpts from U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* ..... App. 53

TABLE OF AUTHORITIES

Page

CASES

Illinois v. Gates, 462 U.S. 213, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983) 7, 15

Maryland v. Garrison, 107 U.S. 79, 107 S.Ct. 1013 (1987) 6

United States v. Grant, 218 F.3d 72 (1st Cir. 2000) 11, 12

United States v. Leon, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984) 9

United States v. Marin-Buitrago, 734 F.2d 889 (2nd Cir. 1984) 9, 10

STATUTES

U.S.C.A. Const. Amend. 4 ..... 1, 7

OTHER AUTHORITIES

U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (July 2002) (http://www.cybercrime.gov/s&smanual2002.htm) 20

PETITION FOR WRIT OF CERTIORARI

CITATION TO REPORTS OF OPINIONS ENTERED

Fifth Circuit Opinion: *U.S. v. Perez*, 484 F.3d 735 (5th Cir. 2007)

District Court Opinion and Order: *U.S. v. Perez*, No. A-05-CR-155-SS (W.D.Tex., filed Sept. 16, 2005)

JURISDICTIONAL STATEMENT

A. The Fifth Circuit affirmed Petitioner's conviction on April 11, 2007.

B. The Fifth Circuit denied Petitioner's petition for panel rehearing on May 29, 2007.

C. This Court has jurisdiction under 28 U.S.C. §1254(1) because judgment has been entered by a federal court of appeals.

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

STATEMENT OF THE CASE

A. Facts Material to the Question Presented

On June 7, 2004, FBI Special Agent Robert Britt submitted an application and affidavit for a search warrant for Petitioner's residence at 7608 Scenic Brook Drive in Austin, Texas. (Appendix 32). According to the affidavit, Britt obtained information from Ann Miller, an agent in the FBI's Buffalo Division, that led to Britt's belief that Petitioner possessed child pornography in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. (Appendix 33-34). Through the reports of a complainant, Miller had discovered that someone with the Yahoo ID of "famcple" had transmitted child pornography to the complainant via a "web cam." (Appendix 41).

On March 4, 2004, Miller issued an administrative subpoena to Yahoo Incorporated in order to find out all account information for the user of Yahoo ID "famcple." (Appendix 41). Yahoo's response indicated that this username was registered to "Mr. Rob Ram." (Appendix 42). Yahoo also provided IP address information for the account on the dates on which the pornographic materials were transmitted. (Appendix 42). A special agent in the FBI's Buffalo division identified Time Warner Cable as the owner of the IP address that "famcple" had used. (Appendix 43). Subsequently, Time Warner Cable was served with an administrative subpoena regarding the account information for the user of this IP address. (Appendix 43). Time Warner Cable then provided information revealing that Petitioner was the subscriber to the account that was assigned this IP address, and Petitioner's address was 7608 Scenic Brook Drive, Austin, Texas 78736. (Appendix 43).

After verifying that Petitioner lived at 7608 Scenic Brook Drive, Britt concluded that there was probable cause to believe "that a computer(s) located at 7608 Scenic Brook Drive, Austin, Texas 78736, has been used to commit the offense of possession, transmission, and trafficking of child pornography." (Appendix 44).

Regarding the administrative subpoena that was issued to Time Warner Cable, Britt testified that it requested all subscriber account-billing and service-type information for the user of the IP address that had been identified as the source of the unlawful transmissions. (RR I 17). Time Warner Cable's response indicated that Petitioner owned the account, but it also stated that it could provide additional information about Petitioner's account. (RR I 18). Although the information from Yahoo indicated that the user ("famcple") who had transmitted the pornography had a user ID of "stephenmee2003" and listed his full name as "Rob Ram," both of which bear no resemblance to Petitioner's name (Javier Perez), Britt did not request any additional information from Time Warner. (RR I 18).

Upon execution of the warrant, Britt met Edwin Atterberry at the front door. (RR I 10). Atterberry identified himself as Petitioner's roommate, and Britt also discovered that a third roommate lived at the residence. (RR I 10). Britt testified that his conversation with Atterberry led him to modify the search so that it was confined to Petitioner's room and the common areas of the house. (RR I 11). After the law enforcement agents searched Petitioner's room, they asked him whether he had any other child pornography in the house; Petitioner then directed them to storage bins in the garage. (RR I 13).

Britt further testified that if all three of the individuals who resided at Petitioner's house were using the Internet on their separate computers at the same time, their activities would be registered under the same IP address because only one IP address resolves to the modem before the information leaves the house. (RR I 19). Britt also testified that at the time of submitting the search-warrant affidavit to the magistrate judge, he had no reason to believe that there was anyone other than Petitioner living at the house. (RR I 76).

Atterberry testified that he had been living at Petitioner's house for 2.5 years when he was awakened by a knock at the door on June 9, 2004. (RR I 26-27). Atterberry met an FBI agent at the door, and he told the agent that he was renting a room from Petitioner. (RR I 27). The agent then asked whether anyone else lived at the house, and Atterberry responded that Robert Ramos was also renting a room from Perez. (RR I 27). Atterberry testified that "Rob Ram" is short for "Robert Ramos." (RR I 27). Atterberry testified that he next identified his, Petitioner's, and Ramos' bedrooms for the agents. (RR I 27). Also, Atterberry testified that the agents could have seen that wires were running into the three separate bedrooms. (RR I 31). Furthermore, Atterberry testified that there was a sticker in the mailbox that contained the names of the three roommates. (RR I 29). Atterberry also testified that at the time of the search, Ramos had lived at the residence for four years, and he received mail. (RR I 40). Moreover, three or four vehicles were typically parked at the residence. (RR I 40).

Atterberry testified that he did not have a key to Petitioner's room, and he never went inside Petitioner's room without Petitioner. (RR I 35). Likewise, Petitioner

was not permitted to enter Atterberry's or Ramos' respective rooms if either was not present because each bedroom was reserved for each roommate's exclusive use. (RR I 35).

Jeffrey Eckert, who is a sergeant with the Texas Attorney General's Cyber Crimes Unit, testified that he works as a forensic analyst of digital electronic data. (RR I 49, 52). Eckert was involved in the execution of the search warrant on June 9, 2004, and his duty was to seize any electronic or digital evidence that was found at the scene. (RR I 52). Eckert testified that IP addresses are assigned by the Internet Service Provider (ISP), and the law allows an ISP to provide the name, address, and billing information of a subscriber. (RR I 60). Eckert testified that in investigations such as this one, law enforcement agencies typically provide the ISP with a date, time, and IP address; the ISP then provides the subscriber information. (RR I 60). Moreover, Eckert testified that if a router is involved in the Internet connections, all of the connections in the residence resolve back to one IP address regardless of whether the Internet use is within a home or business. (RR I 60-61). Thus, if three people in one household had one Internet-service subscription, the ISP would see all of their activity as one IP address. (RR I 61). Eckert also testified that every computer has a unique IP address to identify itself in an internal network, but when the information leaves the home, the information is identified under the IP address that the ISP assigned to the subscriber. (RR I 61). Eckert reiterated that from an outsider's perspective, there is only one IP address regardless of whether each computer in a house or business has its own unique IP address to identify itself within an internal network. (RR I 61). Eckert testified that the IP address that comes out of the home (*i.e.*, the external IP address) is

not related to the internal IP addresses of the individual computers; instead, the external IP address is the address that the ISP owns and assigns to the subscriber. (RR I 61).

B. Basis for Federal Jurisdiction in the Court of First Instance

The district court had subject-matter jurisdiction because Petitioner was alleged to have violated 18 U.S.C. §2252(a)(4)(B) in the Western District of Texas by possessing compact and floppy disks containing visual depictions of minors engaging in sexually explicit conduct.

C. Proceedings Below

The district court denied Petitioner's motion to suppress. (Appendix 18). In particular, the district court found that Agent Britt's "behavior in obtaining a warrant for the whole house was objectively reasonable and the execution of the warrant only in common areas and [Petitioner's] bedroom aligns exactly with the instructions of the Court in [*Maryland v. Garrison*, 107 U.S. 79, 107 S.Ct. 1013 (1987)]." (Appendix 23).

On appeal, the Fifth Circuit agreed with Petitioner's argument that *Garrison* does not apply because "the officers faced a situation in which they knew that 7608 Scenic Brook Drive contained three residences, and had probable cause to believe that unlawful transmissions were made from one of the residences, but did not know which residence." (Appendix 11). However, the Fifth Circuit held that the officers executing the search warrant did not act unreasonably in continuing the search on Petitioner's property because the new information about multiple residents at Petitioner's house did not undermine

the magistrate's initial probable cause determination. (Appendix 13-14). The Fifth Circuit stated:

> In the instant case, the new information acquired by the police was that [Petitioner's] house contained two other residences in addition to his own. Because the IP address in question was registered in [Petitioner's] name, and because the two other individuals living in [Petitioner's] house maintained separate residences, there was still a fair probability that [Petitioner] was the party responsible for the illegal transmissions.

(Appendix 13-14)

REASONS FOR GRANTING THE WRIT

The Fifth Circuit has decided an important federal question in a way that conflicts with relevant decisions of this Court, as the Fifth Circuit has sanctioned a standard for the issuance of search warrants in cyber-crime cases that ignores the realities of Internet technology and falls below a rational conception of probable cause.

A valid search warrant may only issue upon a finding of probable cause. U.S.C.A. Const. Amend. 4. A magistrate's finding of probable cause is entitled to great deference by reviewing courts, and a magistrate need only have a substantial basis for concluding that a search would uncover evidence of wrongdoing. *Illinois v. Gates*, 462 U.S. 213, 236, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983).

Probable cause is a practical, nontechnical conception. *Gates*, 462 U.S. at 231. In determining whether probable

cause exists to issue a search warrant, the issuing magistrate should be guided by the factual and practical considerations of everyday life on which reasonable and prudent men, as opposed to legal technicians, act:

> The process does not deal with hard certainties, but with probabilities. Long before the law of probabilities was articulated as such, people formulated certain common-sense conclusions about human behavior; jurors as factfinders are permitted to do the same – and so are law enforcement officers. Finally, the evidence thus collected must be seen and weighted not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement. As these comments illustrate, probable cause is a fluid concept – turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules.

Id. at 231-32

An appropriate standard for assessing probable cause is whether there is a "fair probability that contraband or evidence of a crime will be found." *Id.* at 238.

Although reviewing courts give great deference to a magistrate's probable-cause determination, these courts will not approve a warrant based on an affidavit that does not "provide the magistrate with a substantial basis for determining the existence of probable cause." *Id.* at 239. The magistrate's action cannot be a mere ratification of the bare conclusions of others, as the magistrate must be presented with sufficient information to determine whether probable cause exists. *Id.* In order to ensure that a magistrate does not abdicate his duties by merely

ratifying the assertions of law enforcement officers, courts must continue to conscientiously review the sufficiency of affidavits on which warrants are issued. *See id.* Moreover, even if a reviewing court determines that a warrant application was supported by more than a "bare bones" affidavit, the court may properly conclude that, notwithstanding the deference that magistrates deserve, the warrant was invalid because the magistrate's probable-cause determination reflected an improper analysis of the totality of the circumstances. *United States v. Leon*, 468 U.S. 897, 915, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

In the present case, this Court should issue a writ of certiorari because the Fifth Circuit has sanctioned a standard for the issuance of search warrants in cyber-crime cases that falls below the constitutional requirement of probable cause. Unless this Court acts, magistrates will use the Fifth Circuit's opinion as precedent for issuing search warrants based upon affidavits whose facts do not establish probable cause under the totality of the circumstances.

A. The fact that illegal transmissions emanate from an IP address that is registered to a specific person does not establish probable cause to search the registrant's property unless there is evidence that the registrant is the sole user of that IP address.

On direct appeal, Petitioner argued that upon discovery of the fact that multiple people resided at Petitioner's house, the officers executing the search warrant should have ceased its execution and returned to the magistrate with the new information. To support his position, Petitioner relied on *United States v. Marin-Buitrago*, 734 F.2d

889, 894 (2nd Cir. 1984). In that case, the Second Circuit explained that a magistrate, as opposed to an officer executing the search warrant, should determine whether a change in the underlying facts casts doubt on the existence of probable cause:

> The restrictions, however, not only ensure that probable cause continues to exist, but also that it is the neutral magistrate, not the executing officers, who determines whether probable cause continues to exist. Thus, when a definite and material change has occurred in the facts underlying the magistrate's determination of probable cause, it is the magistrate, not the executing officers, who must determine whether probable cause still exists. Therefore, the magistrate must be made aware of any material new or correcting information.

Marin-Buitrago, 734 F.2d at 894

The Fifth Circuit ruled that *Marin-Buitrago* was inapplicable to the present case because the new information about multiple occupants did not bring the level of probability below what was necessary for probable cause. (Appendix 12). The Fifth Circuit's holding ignores the realities of the technology of IP addresses.

In the modern world of wireless Internet access and laptop computers, the association between an IP address and a physical address is not enough to establish probable cause to search a specific person's property. For example, if Petitioner had an unsecured wireless connection, anyone with a laptop computer could have come into the vicinity of Petitioner's residence and transmitted the illegal

materials. Neighbors also would have been able to easily use his Internet access to make the transmissions.[1] Such behavior is not farfetched considering that someone who commits cyber crime might actively attempt to avoid police detection by making illegal transmissions from an IP address that is registered in someone else's name.

The facts in the affidavit supported a finding of probable cause only if a neutral magistrate believed that Petitioner was the sole user of the IP address. Petitioner acknowledges that if the FBI had evidence that he owned the user name "famcple," probable cause would have arisen to search his residence. In *United States v. Grant*, 218 F.3d 72, 73 (1st Cir. 2000), which is one of the only other cases in the federal courts to have dealt with a similar issue, the search-warrant affidavit stated that the defendant was the registered owner of a screen name that possessed child pornography. The defendant argued that this evidence was insufficient to establish probable cause because the affidavit failed to prove that the defendant, as opposed to an imposter, possessed the pornographic materials. *Grant*, 218 F.3d at 75. The First Circuit correctly rejected the defendant's argument:

---

[1] Using someone's unsecured wireless connection requires little knowledge about computers. Most computers that are equipped with wireless cards automatically access the Internet by detecting the nearest wireless signal. As a result, an unscrupulous person can tap into someone else's Internet connection for free, and the activity will be registered to the resident who pays for the Internet connection.

> There is, as [the defendant] urges, always reason to question whether a screen name is actually being used by the individual to whom it is registered. But, as [the defendant] has acknowledged, use of a password-protected account does require, at the least, that the user know the password associated with a given screen name. Though the evidence demonstrates that an individual other than an account's registrant might access that account illicitly, there is no evidence suggesting that on any given occasion, the user is not likely in fact to be the registrant. Thus, even discounting for the possibility that an individual other than [the defendant] may have been using his account, there was a *fair probability* that [the defendant] was the user and that evidence of the user's illegal activities would be found in [the defendant's] home. We therefore reject [the defendant's] argument that evidence of a screen name's activity is, in all cases, per se insufficient to establish probable cause with respect to the registrant.

Id.

The First Circuit's finding of probable cause in *Grant* hinged on the unlikelihood that someone other than the defendant had accessed the defendant's password-protected account. Probable cause existed because a magistrate could reasonably find that if the defendant possessed child pornography on an account that was password protected, then there was a fair probability that the police would find the child pornography on the defendant's computer.

In the present case, however, the affidavit fails to show such an exclusive connection between Petitioner and

the user name ("famcple") that transmitted the child pornography. Based on the facts that were stated in the affidavit, there was not a fair probability that child pornography would be found on Petitioner's property unless the magistrate indulged the assumption that Petitioner was the sole user of the IP address that transmitted the illegal materials. On the other hand, if there was evidence establishing that Perez was the registered owner of the "famcple" user name, then the case would be closer to *Grant*.

B. Once the executing officers discovered that multiple residents lived at Petitioner's residence, they should have discontinued the execution of the search warrant because there was no longer probable cause to search Petitioner's property.

When the FBI agents discovered that multiple occupants used the IP address that was registered in Petitioner's name, the probable-cause determination was undermined, as any of the residents living at Petitioner's property could have been the culprit who sent the illegal transmissions. The agents should have been aware of this possibility, as Sergeant Eckert testified that all Internet activity at Petitioner's residence resolved to one IP address. (RR I 60-61). From an outsider's perspective, the IP address of the unlawful transmissions would have been the same regardless of which resident made the transmissions. (RR I 61).[2]

---

[2] The association between an offending IP address and the registered subscriber to that IP address is not analogous to fingerprint evidence at crime scenes. While a fingerprint is unique to each individual, an IP

(Continued on following page)

The Fifth Circuit found that "the new information acquired by the police was that [Petitioner's] house contained two other residences in addition to his own." (Appendix 13). However, based on the testimony from the hearing on the motion to suppress, there was other material information that the officers should have been required to report to the magistrate: (1) that there were cables running into the separate bedrooms of the two other occupants of Petitioner's house, and (2) one of the occupants was named "Robert Ramos," which was very similar to the name "Rob Ram" that had been listed as the full name of the person who used the offending screen name of "famcple." (RR I 27-31). Although the Fifth Circuit did not comment about the significance of "Robert Ramos," the court found that the existence of wires traveling into each roommate's bedroom added support to the possibility that Petitioner was not the person who made the illicit transmissions. (Appendix 11). Even so, the court failed to find that this information should have been reported to the magistrate.

C. Upon receiving new information from the executing officers, a neutral magistrate would have concluded that there was no longer probable cause to search Perez's property.

Information that two other residents rented bedrooms at the residence would have led a neutral magistrate to ask for more information before signing off on a warrant

---

address simply marks the source of transmissions. Multiple people can use the same IP address, and there is no way to know whether the registered subscriber of that IP address was the culprit who made illegal transmissions.

that isolated the search to Petitioner's exclusive property. Britt and Eckert testified that the IP address emanating from Petitioner's residence would have been the same regardless of which roommate made the illicit transmissions. As a result, the fact that three people resided at the house reveals that there was only a 33 percent chance that Petitioner was the person who transmitted the unlawful images. Although Petitioner acknowledges that quantifying probable cause can be a slippery practice, 33 percent should not be considered a "fair probability that contraband or evidence of a crime will be found" on Petitioner's property. *See Illinois v. Gates*, 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983).

Although Petitioner believes that the mere fact that multiple people used the same IP address as Petitioner should have been enough to undermine the magistrate's probable-cause determination, information about the cables running into each resident's room cast further doubt on the existence of probable cause to search Petitioner's property, as this fact confirmed that Petitioner was not the only person at the property who used the Internet. Even more importantly, the fact that a "Robert Ramos" lived at the residence should have triggered alarm bells in the heads of both the magistrate and executing officers, as an administrative subpoena revealed that the screen name ("famcple") that sent the unlawful transmissions was registered to a "Mr. Rob Ram." At the very least, a neutral magistrate would have asked the officers to investigate Ramos' connection to the "famcple" screen name before issuing a search warrant for Petitioner's property.

D. The Fifth Circuit has sanctioned a standard of probable cause in the realm of cyber-crime search warrants that violates basic notions of fairness, as innocent landlords and employers will be the subject of intrusive search warrants unless the Supreme Court acts.

This case illustrates policy reasons why the officers should have conducted a further investigation prior to obtaining a search warrant for Petitioner's residence, but because of the Fifth Circuit's ruling, such *de minimus* investigative work will continue in the cyber-crime arena. The person who transmitted the child pornography was registered as "Rob Ram" on the Yahoo website. A few inquiries into the names of Petitioner's roommates would have shown the officers that one of the roommates was named "Robert Ramos." Such a discovery would have led the officers to target Ramos, who was the true culprit in this case.[3] This information was not difficult to obtain, as Petitioner's other roommate, Edwin Atterberry, testified that each of the roommates' names was printed on a sticker inside of their common mailbox. (RR I 29). Also, the fact that cables ran into each of the three separate bedrooms of the residence would have alerted a neutral magistrate that there were three people using the same IP address at Petitioner's residence. Considering that the sole basis for the magistrate's initial probable-cause determination was the link between the IP address and the

---

[3] Perez acknowledges that he was caught with child pornography, but he submits that the mere act of possession is less culpable than Ramos' act of transmitting images and videos to people over the Internet. Significantly, Perez was not charged with making unlawful transmissions, which is evidence that the agents realized that he was not the person who made the transmissions to the complainant.

Petitioner's physical address of 7608 Scenic Brook Drive, the revelation that Petitioner was not the only person residing at the property should have led the magistrate to ask for more information from the investigators prior to issuing the search warrant.

If this Court denies a writ of certiorari, then magistrates will continue to issue search warrants based upon the mere association between IP address registration and illegal activity emanating from that IP address, even if multiple people use the same IP address. Under the Fifth Circuit's holding, when tenants rent a house from a landlord who registers Internet service in the landlord's name, the tenants can commit countless computer crimes, and the landlord will always be the person who is named in the search warrant. Likewise, employers who register for Internet service will be held accountable for rogue employees' illicit conduct.[4]

Cyber crime is a relatively new area of the law, and this Court should take this opportunity to preserve individual liberties while encouraging diligent investigations. This case is marred by minimal investigative work because the officers believed that they merely needed information that connected a particular IP address to a particular residence. As this case illustrates, this circumstantial

---

[4] Petitioner does not know how the Supreme Court registers its IP address, but Petitioner suspects that there is not a separate IP address for each employee. The honorable judges and clerks should simply go to "whatismyipaddress.com" to discover their respective IP addresses, and they will likely find an overlap. If a rogue law clerk were to send out unlawful transmissions from the Court's computers, would this Court believe it fair for the registered subscriber of the Court's IP address to be the subject of a search warrant, even though this subscriber had nothing to do with the transmissions?

evidence, standing alone, should not be enough to establish probable cause when more than one person uses the Internet at a residence or place of employment. A denial of a writ of certiorari would mean that countless landlords or business owners who register Internet service in their names can be searched for conduct committed by tenants or employees. Also, now that such landlords and business owners are subject to such search warrants based on other people's crimes, they can only protect themselves by installing monitoring software so that they can be aware of the Internet activity that occurs on their respective IP addresses. Such a measure would infringe upon people's privacy expectations with regard to their Internet activity, and it would prove costly for the person who must integrate the software into a computer network. The Fifth Circuit seems unaware of the import of its holding, as the opinion fails to mention these onerous consequences of its decision.

A possible reason why the Fifth Circuit and the district court might have upheld the search in the present case is that they did not completely grasp the technology of IP addresses. At the hearing on the motion to suppress evidence, the district judge casually dismissed Petitioner's argument regarding the fact that multiple people used the same IP address: "You know, I have two web addresses in my home. My wife and I have separate ones. We have six children, thank God, are all gone, but I rather suspect that they would have separate addresses." (Appendix 50-51). This quote reveals that the district judge might have confused IP addresses with e-mail addresses, and it demonstrates his failure to understand the technical testimony at the hearing, as Sergeant Eckert had testified that even if people have separate computers at a residence, all of the

Internet activity resolves to one IP address before leaving the residence. (RR I 61).

Moreover, this Court will not cripple Government investigations by ruling that probable cause was absent in the present case. Instead, such a ruling will give the Government an incentive to conduct more investigative work in order to find the true culprit. All that Britt needed to do in this case was check the mailbox at Petitioner's residence, and he would have seen that Robert Ramos and Edwin Atterberry also lived there. (RR I 29). The name "Robert Ramos" would have tipped Britt that Ramos was the likely transmittor of the pornographic materials, as Britt had already known that the culprit's registered name on the Yahoo account was "Mr. Rob Ram." The price of this extra bit of investigative work is low in relation to the value of the Constitutional right to be free from unlawful searches and seizures.

Finally, even the United States Department of Justice has stated that the mere association of an IP address with illegal activity emanating from that address should not be enough to establish probable cause to search a person's property:

> Probable cause challenges may also arise when supporting evidence in an affidavit derives heavily from records of a particular Internet account or Internet Protocol ("IP") address. The problem is a practical one: generally speaking, the fact that an account or address was used does not establish conclusively the identity or location of the particular person who used it. As a result, an affidavit based heavily on account or IP address logs must demonstrate a sufficient connection between the logs and the location to be searched to

> establish "a fair probability that contraband or evidence of a crime will be found in [the] particular place" to be searched.

U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, at II-C-2 (July 2002) (http://www.cybercrime.gov/s&smanual2002.htm) (Appendix 56-57)

If the Department of Justice questions whether the mere association between illegal activity and an IP address is enough to establish probable cause to search the registrant's property, then it seems profoundly unfair for the Fifth Circuit to hold otherwise. This Court should exercise its jurisdiction to clarify the probable cause determination in the realm of Internet crime.

Respectfully submitted,

CHRISTOPHER M. PERRI
2906 N. Broadway, #3
Chicago, IL 60657
(773) 868-0360
Fax No. (512) 474-8252
Texas Bar Number:
24047769

JOSEPH A. TURNER
(*Counsel of Record*)
1504 West Ave.
Austin, TX 78701
(512) 474-4892
Fax No. (512) 474-8252
Texas Bar Number:
20322500

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 06-50041

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

JAVIER PEREZ,

Defendant-Appellant

Appeal from the United States District Court
for the Western District of Texas

(Filed April 11, 2007)

Before KING, GARZA and PRADO, Circuit Judges.

PRADO, Circuit Judge:

Defendant-Appellant Javier Perez ("Perez") was convicted of possession of child pornography and sentenced to fifty-seven months imprisonment. Perez appeals the district court's order denying his motion to suppress evidence acquired in a search of his premises on June 9, 2004. Perez also appeals the enhancement of his sentence based on his possession of images depicting prepubescent minors and images depicting sadistic/masochistic conduct. For the reasons that follow, we affirm.

I. FACTUAL AND PROCEDURAL BACKGROUND

In March 2004, a woman in Jamestown, New York, complained to the police that she had received an internet message from someone with the Yahoo ID "famcple," who proceeded to show her images of young children engaged in sexual acts. This complaint was forwarded to the Buffalo, New York division of the Federal Bureau of Investigation ("FBI"). The FBI sent a subpoena to Yahoo! Incorporated ("Yahoo") seeking information regarding the user of Yahoo ID "famcple." Yahoo responded with information that the user's login name was "stephenmee2003," that the user's full name was "Mr. Rob Ram," and that on the dates when the child pornography was transmitted, the user had been using the IP address 24.27.21.6.

The FBI determined that the owner of the IP address 24.27.21.6 was Time Warner Cable ("Time Warner"). After being served with a subpoena, Time Warner informed the FBI that the IP address in question was assigned to Javier Perez, residing at 7608 Scenic Brook Drive, Austin, Texas 78736. The FBI performed a public records check, a utilities company check, and an internet white pages check, all of which indicated that there was a Javier Perez living at 7608 Scenic Brook Drive, Austin, Texas 78736. Special Agent Robert W. Britt ("Britt") of the FBI sought a warrant to search that address. On June 1, 2004, a United States Magistrate Judge issued a warrant authorizing the search of the "residence, business, outbuildings, and motor vehicles on the curtilage located at: 7608 Scenic Brook Drive, Austin, TX 78736."

On June 9, 2004, Britt and other officers executed the search warrant. When the officers arrived at the front door of 7608 Scenic Brook Drive, they were met by Edwin

Atterbury ("Atterbury"), who explained that he was a housemate of Perez and that a third person also resided in the house.[1] Britt proceeded with the search but confined it to Perez's room and the common areas of the house. After the officers searched Perez's room, in which they located compact discs containing child pornography, Perez, who was present during the search, directed the officers to storage bins in the garage, where more such compact discs were found. In total, approximately 4000 compact discs containing thousands of images of child pornography were seized by the officers.

A grand jury indictment returned on July 19, 2005, charged Perez with one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). Perez moved to suppress the evidence seized from his premises during the June 9, 2004 search. After a hearing on September 15, 2005, the district court denied Perez's motion. Perez then entered a conditional guilty plea, retaining his right to appeal the district court's ruling on his motion to suppress. On December 9, 2005, the district court sentenced Perez to fifty-seven months in federal prison followed by seven years of supervised release. Perez now appeals.

II. JURISDICTION

This is an appeal from a final judgment of a district court in a criminal case. This court has jurisdiction pursuant to 28 U.S.C. § 1291.

---

[1] Britt testified that he left the house before discovering that the third housemate's name was Robert Ramos, suspiciously similar to the name provided by Yahoo, "Mr. Rob Ram."

III. ANALYSIS

A. The district court did not err in denying Perez's motion to suppress

1. Standard of Review

When reviewing the denial of a motion to suppress evidence, this court reviews the district court's factual findings for clear error and the district court's conclusions regarding the sufficiency of the warrant and the constitutionality of law enforcement action de novo. *United States v. Cherna,* 184 F.3d 403, 406 (5th Cir. 1999).

2. Perez's Arguments

Perez argues that the district court should have granted his motion to suppress the evidence seized during the search of his premises on June 9, 2004. Perez first insists that there was insufficient probable cause to support the issuance of a search warrant. Perez alleges that "mere association between an IP address and a physical address is insufficient to establish probable cause." Even if the initial determination that probable cause existed was reasonable, however, Perez argues that "[t]he discovery that multiple people resided at Perez's residence undermined the basis for the magistrate's probable-cause determination." Perez argues that the officers' discovery of Perez's housemates should have indicated to them that there was no longer probable cause to believe that Perez was the source of the unlawful transmissions. He further argues that the existence of these two housemates was material information that the officers had a duty to report to the issuing magistrate. Finally, Perez argues that the good-faith exception does not apply because the officers' reliance on the warrant was

no longer objectively reasonable once they discovered that two other persons lived with Perez at 7608 Scenic Brook Drive.

3. Guiding Supreme Court Precedent

Like this case, *Maryland v. Garrison,* 480 U.S. 79 (1987), involved the constitutionality of a search executed pursuant to a warrant authorizing the search of a structure that turned out to contain more individual residences than was believed at the time the warrant was issued. In *Garrison,* Baltimore police obtained a warrant to search the "third floor apartment" of 2036 Park Avenue. *Id.* at 80. When applying for the warrant and when executing it, police reasonably believed that the third floor of that address had only one apartment and that this apartment was occupied by the suspect McWebb. *Id.* at 81. In the course of their search, the police realized that the third floor actually contained two apartments, and that they were in the process of searching the apartment of Garrison. *Id.* The officers ceased their search of Garrison's quarters, but the contraband they had discovered before doing so became the basis for Garrison's conviction. *Id.* at 80-81. The Supreme Court held that under the circumstances presented, the seizure of contraband from Garrison's apartment did not violate the Fourth Amendment. *Id.* at 88.

While the instant case is not identical to *Garrison* in all relevant particulars, *Garrison* does lay out a framework for how the analysis of this case should proceed. There, the Supreme Court stated that "[i]n our view, the case presents two separate constitutional issues, one concerning the validity of the warrant and the other

concerning the reasonableness of the manner in which it was executed." *Id.* at 84. Perez's appeal presents the same two overarching issues.

4. Validity of Warrant to Search 7608 Scenic Brook Drive

A valid search warrant may be issued only upon a finding of probable cause. *United States v. Brown,* 941 F.2d 1300, 1302 (5th Cir. 1991). The information necessary to show probable cause must be contained within a written affidavit given under oath. *Id.* Probable cause does not require proof beyond a reasonable doubt; a magistrate need only have a substantial basis for concluding that a search would uncover evidence of wrongdoing. *Id.* A magistrate's determination is entitled to deference by reviewing courts. *Id.*

In this case it is clear that there was a substantial basis to conclude that evidence of criminal activity would be found at 7608 Scenic Brook Drive. The affidavit presented to the magistrate included the information that the child pornography viewed by the witness in New York had been transmitted over the IP address 24.27.21.6, and that this IP address was assigned to Javier Perez, residing at 7608 Scenic Brook Drive, Austin, Texas 78736. Perez argues that the association of an IP address with a physical address does not give rise to probable cause to search that address. He argues that if he "used an unsecure wireless connection, then neighbors would have been able to easily use [Perez's] internet access to make the transmissions." But though it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained likely that the source of the transmissions was inside that residence. *See United*

States v. Grant, 218 F.3d 72, 73 (1st Cir. 2000) (stating that "even discounting for the possibility that an individual other than [defendant] may have been using his account, there was a *fair probability* that [defendant] was the user and that evidence of the user's illegal activities would be found in [defendant's] home") (emphasis in original).[2] "[P]robable cause does not require proof beyond a reasonable doubt." *Brown,* 941 F.2d at 1302.

Perez also argues that evidence that illicit transmissions were made does not give rise to probable cause that physical evidence would be located at the residence. However, the New York witness stated that the images she observed appeared to be videos played on a television screen transmitted via a web cam. There was therefore a basis to believe that the suspect would have such videos in his residence. Moreover, Britt stated in his affidavit that, in his experience, persons interested in child pornography typically retain numerous images of child pornography as well as "material documenting the arrangements, the introduction, and tasks to consummate the acquisition of child pornography." Based on this information, there was probable cause to believe that physical evidence of violations of the child pornography laws would be located at 7608 Scenic Brook Drive.

The analysis is complicated, however, by the fact that 7608 Scenic Brook Drive has more than one occupancy unit.[3] The Fourth Amendment requires that a warrant

---

[2] The evidence in *Grant* involved a screen name rather than an IP address, but the principle is equally applicable to the latter.

[3] The government does not contest Perez's claim that he and his housemates each maintained a separate residence within 7608 Scenic Brook Drive.

"particularly describ[e] the place to be searched and the persons or things to be seized." Multiple circuit courts have held that to satisfy the particularity requirement when a search involves a building with multiple, separate residency units, the warrant must specify the precise unit that is the subject of the search. *See United States v. White,* 416 F.3d 634, 637 (7th Cir. 2005). "[W]hen a building is divided into more than one residential unit, a distinct probable cause determination must be made for each unit." *United States v. Butler,* 71 F.3d 243, 249 (7th Cir. 1995); *see also United States v. Hinton,* 219 F.2d 324, 325-26 (7th Cir. 1955) ("For purposes of satisfying the Fourth Amendment, searching two or more apartments in the same building is no different than searching two or more completely separate houses. Probable cause must be shown for searching each house or, in this case, each apartment."). Thus the general rule is that a warrant that authorizes the search of an undisclosed multi-unit dwelling is invalid. *United States v. Gilman,* 684 F.2d 616, 618 (9th Cir. 1982).

There are, of course, exceptions to this rule. The warrant of a multi-unit structure will be valid where (1) there is probable cause to search each unit;[4] (2) the targets of the investigation have access to the entire structure; or (3) the officers reasonably believed that the premises had only a single unit. *United States v. Johnson,* 26 F.3d 669, 694 (7th Cir. 1994); *Garrison,* 480 U.S. at 85-86. *Gilman,*

[4] While this has been stated by the Seventh and Ninth Circuits as an exception, it is perhaps better understood as an application of the general rule that probable cause must exist for each unit of a multi-unit structure.

684 F.2d at 618.[5] In assessing whether any of these exceptions can support the validity of the warrant, we must look to the information in possession of the police and magistrate at the time the warrant was issued. *Garrison,* 480 U.S. at 85 ("The validity of the warrant must be assessed on the basis of the information that the officers disclosed, or had a duty to discover and disclose, to the issuing Magistrate.").

In *Garrison,* the Supreme Court concluded that the warrant to search the third floor of 2036 Park Avenue was valid because the police reasonably believed that the third floor contained only one apartment when they applied for the warrant. Though the Court acknowledged that "[a]rguments can certainly be made that the police in this case should have been able to ascertain that there was more than one apartment on the third floor of this building," the Court noted that the police "made specific inquiries to determine the identity of the occupants of the third-floor premises," including visiting the address and checking with the local gas and electric company and local police department. *Id.* at 86 n.10.

Though Perez contends that the police performed an insufficient investigation into the occupancy of 7608 Scenic Brook Drive before obtaining the warrant, the steps that the police took in this case are similar to those taken in

---

[5] There is also authority for the proposition that a warrant to search a multi-unit dwelling is valid if it specifies the name of the occupant of the apartment against which it is directed, despite the absence of any physical description of the particular apartment. *United States v. Bedford,* 519 F.2d 650, 655 (3d Cir. 1975). In this case, however, the search warrant did not include Perez's name, so this exception is not applicable.

Garrison. The officers performed a public records check, a utilities company check, and an internet white pages check, all indicating that 7608 Scenic Brook Drive was occupied by Perez and none indicating the presence of any other residents. We therefore conclude that the police officers reasonably believed that 7608 Scenic Brook Drive had only one resident at the time the warrant was issued. Accordingly, the warrant in this case was valid.

5. Reasonableness of Search of 7608 Scenic Brook Drive

Garrison next counsels us to examine "whether the execution of the warrant violated [the defendant's] constitutional right to be secure in his home." 480 U.S. at 86. In that case, the Supreme Court concluded that the police did not violate Garrison's rights, because as soon they "discovered that there were two separate units on the third floor and therefore were put on notice of the risk that they might be in a unit erroneously," they ceased to search that unit. *Id.* at 87. The Court wrote that "[i]f the officers had known, or should have known, that the third floor contained two apartments before they entered the living quarters on the third floor, they would have been obligated to limit their search to McWebb's apartment." *Id.* at 86. In this case, the district court concluded and the government now maintains that *Garrison* squarely supports the officers' actions in executing their search of 7608 Scenic Brook Drive. When, upon arriving at the house, the officers learned that it contained three residences, the officers confined their search to areas used by Perez. This, the government argues, is exactly what *Garrison* prescribes.

As Perez points out, however, this case is not precisely like *Garrison*. In this case, the discovery of additional residents of 7608 Scenic Brook Drive also altered the calculation of probable cause against Perez. The discovery of the two other housemates should have alerted the police to the possibility that one of the other housemates might have been using the IP address in question at the time of the illicit transmissions. The existence of wires traveling into each of the bedrooms added support to that possibility. Indeed, once the officers learned of the additional residents, the situation resembled one that *Garrison* explicitly declined to address:

> We expressly distinguish the facts of this case from a situation in which the police know there are two apartments on a certain floor of a building, and have probable cause to believe that drugs are being sold out of that floor, but do not know in which of the two apartments the illegal transactions are taking place. A search pursuant to a warrant authorizing a search of the entire floor under those circumstances would present quite different issues from the ones before us in this case.

480 U.S. at 89 n.13. Here, the officers faced a situation in which they knew that 7608 Scenic Brook Drive contained three residences, and had probable cause to believe that unlawful transmissions were made from one of the residences, but did not know which residence. *Garrison* does not assist us in resolving this problem.

Perez maintains that when the officers acquired information that altered the probable cause determination, they had a duty to present this information to the magistrate. Because they did not do so, he claims, their

search of his premises was unreasonable. There are no Fifth Circuit decisions that directly address this issue. Perez relies on *United States v. Marin-Buitrago,* 734 F.2d 889, 894 (2d Cir. 1984), where the Second Circuit declared that "when a definite and material change has occurred in the facts underlying the magistrate's determination of probable cause, it is the magistrate, not the executing officers, who must determine whether probable cause still exists. Therefore, the magistrate must be made aware of any material new or correcting information."

When this decision is read in full, however, it becomes clear that *Marin-Buitrago* does not support Perez's position that the evidence from his residence must be suppressed. Therein, the Second Circuit indicated that the evidence resulting from the search should be suppressed only when the new information brought the level of probability below what was necessary for probable cause. Thus the court stated that "[i]n determining on this appeal whether the affidavit still supports a finding of probable cause after the inclusion of [the new information], we must assume the role of the issuing magistrate." *Id.* at 895. After concluding that "[e]ven with the supplemental information, the affidavit clearly establishes, by a fair probability," that the search would produce evidence of narcotics, and that therefore "the warrant for the search . . . was supported by probable cause at the time it was executed," the court upheld the district court's denial of the defendant's motion to suppress. *Id.* at 896.

The Sixth Circuit has reached the same result through slightly different reasoning. In *United States v. Bowling,* 900 F.2d 926, 933 (6th Cir. 1990), the Sixth Circuit commented that:

> The Supreme Court has emphatically cautioned that in the absence of urgent circumstances officers should not rely on their own discretion, but should instead resort to a neutral magistrate, to determine whether probable cause to conduct a search exists. *See Johnson v. United States,* 333 U.S. 10, 14 (1948). . . . Although *Johnson*'s admonition speaks specifically to the situation in which officers conduct a warrantless search, we think it is equally applicable to cases in which officers possess a warrant but are alerted to circumstances which affect the probable cause for its execution.

Addressing the case before it, the Sixth Circuit stated that "[b]ecause no exigent circumstances are presented by the facts of this case, the officers should have refrained from the second search until a neutral magistrate determined that probable cause continued to exist." *Id.* However, the court went on to declare, citing *Franks v. Delaware,* 438 U.S. 154, 171-72 (1978), that "[n]otwithstanding the officers' failure to [return to the magistrate], the fruits of the second search are not to be suppressed if this court finds that a neutral magistrate would have determined that probable cause existed." *Id.* Concluding that a neutral magistrate apprised of the new information would still have found that probable cause existed, the court declined to suppress the fruits of the search. *Id.* at 934.

In the instant case, the new information acquired by the police was that Perez's house contained two other residences in addition to his own. Because the IP address in question was registered in Perez's name, and because the two other individuals living in Perez's house maintained separate residences, there was still a fair probability that Perez was the party responsible for the illegal

transmissions. This court has held that "the requisite 'fair probability' is something more than a bare suspicion, but need not reach the fifty percent mark." *United States v. Garcia,* 179 F.3d 265, 269 (5th Cir. 1999) (citing *United States v. Antone,* 753 F.2d 1301, 1304 (5th Cir. 1985)); *see also Texas v. Brown,* 460 U.S. 730, 742 (1983) (stating that probable cause "does not demand any showing that such a belief be correct or more likely true than false"). Accordingly, we find that even in light of the new information regarding Perez's housemates, probable cause still existed for the search of Perez's premises. As a result, the district court did not err by refusing to suppress the fruits of the officers' search of Perez's premises.

B. The district court did not err in enhancing Perez's sentence based on his possession of images depicting prepubescent minors and images depicting sadistic/masochistic conduct

1. Standard of Review

Perez objected at trial to the enhancement of his sentence for possession of images depicting prepubescent children and images depicting sadistic or masochistic conduct. The nature of his objection was that because he had not been indicted for or pled guilty to possessing these materials, any increase in offense level on this basis would be a violation of his Sixth Amendment rights. At Perez's sentencing hearing, his lawyer characterized these objections as "*Booker* objections." On appeal, however, Perez objects to these sentencing enhancements on the basis that there is insufficient proof that he intended to possess materials of this nature.

Because Perez did not argue before the district court the specific objection that he now raises, we analyze his claim under the plain error framework set out by the Supreme Court in *United States v. Olano,* 507 U.S. 725 (1993). Under plain error review, we may overturn a district court decision only if there is (1) error, (2) that is plain, and (3) that affects substantial rights. *United States v. Mares,* 402 F.3d 511, 520 (5th Cir. 2005) (quoting *United States v. Cotton,* 535 U.S. 625, 631 (2002)). "If all three conditions are met an appellate court may then exercise its discretion to notice a forfeited error but only if (4) the error seriously affects the fairness, integrity, or public reputation of judicial proceedings." *Id.*

2. Applying Plain Error Review

Relying on *United States v. Kimbrough,* 69 F.3d 723 (5th Cir. 1995), Perez argues that the Fifth Circuit requires that the government prove intent to possess images depicting prepubescent children or sadistic/masochistic conduct to obtain sentencing enhancements under U.S.S.G. §§ 2G2.2(b)(1) and 2G2.2(b)(3). Addressing sentencing enhancements under these provisions, the *Kimbrough* court stated that "the trial court heard sufficient evidence . . . to conclude that Kimbrough intentionally ordered and possessed child pornography which depicted prepubescent minors or minors under the age of 12, or, at the very least, had reckless disregard of the age of the performers" and that "the trial court heard sufficient evidence at trial to conclude that Kimbrough intentionally ordered and possessed pornography which depicted sadistic or masochistic conduct." 69 F.3d at 734. We can conclude from these quotations that this circuit requires a showing of either reckless disregard or intent

for sentencing enhancements under U.S.S.G. §§ 2G2.2(b)(1) and 2G2.2(b)(3).

Perez argues that language used by the district court indicated that the court "used a strict liability theory in assessing whether the enhancement provisions applied to Perez." The language used by the district court in discussing these enhancements at Perez's sentencing hearing is ambiguous. But even if the district court did commit error, this error did not affect Perez's substantial rights, for there is sufficient evidence to support the enhancements under the correct standard.

Perez admitted that he possessed and "collected" child pornography. He was able to direct the officers searching his home to compact discs that contained child pornography. At least one such compact disc had file folders labeled "kiddie porn." The Attorney General's office reviewed only a portion of the approximately 4000 compact discs seized from Perez, and still found an estimated 2500 images of child pornography. Numerous of these images involved either prepubescent children or sadistic/masochistic conduct. While Perez claims that he did not look at most of the child pornography files he downloaded, he admits having seen some of them. Moreover, the downloaded files often had file names that summarized their images, implying that Perez could have been aware of the contents even without viewing each image. Accordingly, there is sufficient evidence in the record to demonstrate that Perez either intended to possess prepubescent and sadistic/masochistic images or had reckless disregard for his possession of them. We therefore affirm the district court's enhancement of Perez's sentence.

IV. CONCLUSION

For the reasons stated above, we affirm Perez's conviction and sentence.

AFFIRMED.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA

-vs- **CAUSE NO. A-05-CR-155-SS**

JAVIER PEREZ

ORDER

(Filed Sep. 16, 2005)

Before the Court are Defendant Javier Perez's Motion to Suppress [#9], the Government's response, filed September 15, 2005, and Defendant's Supplemental Motion to Suppress [#14]. On September 15, 2005, the Court held a hearing in this matter, and the parties appeared through counsel of record. After considering evidence presented at the hearing, the arguments of the parties, the relevant law, and the file as a whole, the Court made oral factual findings and denied Defendant's Motion to Suppress [#9] in open court on September 15, 2005 and now confirms the same.

I. Factual Background

On June 7, 2004, U.S. Magistrate Judge Robert Pitman issued a search warrant for the residence, business, outbuilding, and vehicles located at 7608 Scenic Brook Drive, Austin, Texas 78736 (7608 Scenic Brook Drive). The warrant issued based on the affidavit of Federal Bureau of Investigation (FBI) Special Agent Robert W. Britt, who sought to search the residence based on information officially supplied to him by Special Agent

Ann M. Miller of the FBI's Buffalo, New York Division. Special Agent Miller had obtained incriminating evidence front Amanda Decker of Jamestown, New York, a witness who had been shown over the internet videos of children engaged in sexual acts by a person whose Yahoo username was "famcple."

An administrative subpoena was sent to Yahoo! Incorporated (Yahoo) on March 5, 2004, asking for any and all subscriber, account, and internet protocol (IP) history information for the Yahoo username "famcple." On March 18, 2004, Yahoo responded, providing the login name "stephanmee2003" for the account and the owner name as "Rob Ram" of Beverly Hills, CA.[1] However, the IP address information of "24.27.21.6" that Yahoo provided for the dates between February 18, 2004 and March 8, 2004 indicated that Time Warner Cable owned the IP address. In response to an administrative subpoena, Time Warner Cable provided the name Javier Perez, and the address 7608 Scenic Brook Drive, Austin, Texas 78736, as the owner of the Roadrunner account that corresponded to the IP address. The FBI later conducted a credit check through Choicepoint, a utilities company check, and an internet white pages check, all of which revealed that Javier Perez lived at 7608 Scenic Brook Drive, Austin, Texas 78736.

The search warrant was executed on June 9, 2004. Prior to and on June 9, 2004, the Defendant was living with two house mates, Edwin Lee Atterberry Jr. and

---

[1] The Government states in its response that it is not uncommon for collectors, purveyors and traders of child pornography to initiate Yahoo email accounts by providing false and/or fictitious names and information. Gov'ts Resp. at 1.

Roberto (or Robert) Ramos, who rented rooms from him. When the officers arrived at 7608 Scenic Brook Drive with their search warrant, Mr. Atterberry answered the door. He told the officers that he lived there along with Perez and told them which bedroom belonged to Perez. The officers approached and knocked on Perez's bedroom door, which was locked. The officers report that after hearing movement in the bedroom without any opening of the door, they forced the door open and located Perez. Evidence consisting of approximately 3,999 compact discs (cds) containing approximately four million images of adult and child pornography was seized from Perez's bedroom and the garage. The officers searched only Perez's bedroom and the common areas of the house for evidence; Atterberry's and Ramos's rooms were not searched.[2] After the officers located Perez, they questioned him in the kitchen, and he led them to at least two plastic tubs full of cds in the garage. There was no evidence presented in the motion or the hearing to challenge the voluntariness of Perez's statements to the officers on June 9, 2004.

At the hearing Special Agent Britt testified that prior to June 9, 2004, he had no knowledge or reason to believe that anyone else but Javier Perez lived at 7608 Scenic Brook Drive. Sergeant Jeffrey Eckert of the Texas Attorney General's office, who participated in executing the search warrant, also testified that he had never been to 7608 Scenic Brook Drive before June 9, 2004, and that it appeared to him to be a residential home in a residential

---

[2] An FBI agent testified at the hearing that agents did enter the rooms of Ramos and Atterberry, but only as a protective sweep to determine that there were no other persons in the house. No evidence was taken from either of these rooms.

neighborhood when he first saw it. Both the defense and the Government submitted photographs of the exterior and interior of the single-story residential house into evidence at the hearing. Def.'s Ex. 2-12, Gov'ts Ex. 1-9. Edwin Lee Atterberry, Jr. took the stand and testified that each of the three men living in the house had his own private bedroom with a lock on the outside of the door and that the men were unrelated adults whose bedrooms were for their own exclusive personal use.

II. Discussion

Defendant files this motion to suppress, alleging his residence was searched without probable cause and without a valid warrant. In response, the Government contends the officers executing the warrant had probable cause to search the residence for evidence of sexual exploitation of minors, and that the search and seizure were within the constitutional boundaries of Fourth Amendment jurisprudence. Defendant attacks the search and seizure on two main grounds: (1) that a separate warrant should have been obtained before Defendant's bedroom was searched; and (2) that the affidavit which provided the basis for the warrant contained a false statement made with reckless disregard for the truth. The Court wholly rejects Defendant's motion. The facts of this case, based on the pleadings and the credible testimony of Special Agent Britt and Sergeant Jeffrey Eckert clearly show that the search was validly executed and was conducted pursuant to a valid search warrant that was based on an affidavit containing accurate information. Alternatively, the Court finds that any error in the execution of the warrant falls within the good faith exception.

A. Probable Cause

First, the Court addresses the issue of probable cause. A valid search warrant may be issued only upon a finding of probable cause. The information necessary to show probable cause must be contained within a written affidavit given under oath. *United States v. Brown*, 941 F.2d 1300, 1302 (5th Cir. 1991). "It is clear that probable cause does not require proof beyond a reasonable doubt; 'only the probability, and not a prima facie showing, of criminal activity is the standard of probable cause.'" *Id.* (*quoting Spinelli v. United States*, 393 U.S. 410, 419 (1969)). The issuing magistrate's determination is entitled to great deference by reviewing courts; the magistrate need only have "a substantial basis for concluding that a search would uncover evidence of wrongdoing." *Id.*

This Court finds that the affidavit of Special Agent Britt established probable cause to search 7608 Scenic Brook Drive. Britt based his affidavit testimony on accurate information he obtained from the Buffalo Division of the FBI, and, further, he confirmed that Perez resided at 7608 Scenic Brook Drive by doing utilities, credit, and interact searches before applying for the warrant. The information provided by Amanda Decker, Yahoo, and Time Warner, collectively resulted in the probability that criminal activity was taking place at 7608 Scenic Brook Drive. This Court finds that the information contained in the affidavit provided the magistrate with a substantial basis for concluding that a search would uncover evidence of criminal activity.

B. Multiple Occupancy Residence

Secondly, Defendant claims that the search was invalid because a second warrant should have been obtained to search Javier Perez's bedroom when the officers realized there were other unrelated adults living in the house with him. The U.S. Supreme Court applies an "objective reasonableness" standard to judge whether the location stated in a search warrant is overly broad. In *Maryland v. Garrison*, 480 U.S. 79 (1987), police officers obtained a search warrant for the entire third floor of a building, not knowing that there were actually two separate apartments on the third floor. The officers seized evidence from the "wrong" apartment before realizing their error, upon realizing, they immediately ceased their search and moved on to the targeted apartment. The Supreme Court held that where the officers' failure to realize the overbreadth of the warrant was objectively reasonable, no Fourth Amendment violation occurred so long as officers thereafter confined their search to the residence of the suspect. *Id.* at 86-88.

As their credible testimony at the hearing indicated, neither Britt nor Eckert knew that there were other residents of the house besides Perez before they arrived to execute the warrant. Because Special Agent Britt did not know there were separate living quarters within the house when he obtained the search warrant, his behavior in obtaining a warrant for the whole house was objectively reasonable and the execution of the warrant only in common areas and Mr. Perez's bedroom aligns exactly with the instructions of the Court in *Garrison*.

Defendant cites *United States v. Greathouse* in his motion for the proposition that a second search warrant

should have been obtained to search Perez's bedroom. 297 F. Supp. 2d 1264 (D. Or. 2003). In *Greathouse*, another child pornography case involving computers, the Court stated as an alternative basis for suppressing the evidence seized that when the officers realized that there were nonfamilial people sharing a house and saw a Do Not Enter sign[3] on the defendant's door, they should have secured the area and obtained a telephonic warrant. *Id.* at 1274-75. However, the Court finds this case distinguishable on several bases. In *Greathouse*, it was a renter, not the owner of the house, whose bedroom was searched. Here, Perez was the owner of the house and the only person individually named by the FBI in their search warrant affidavit. Gov'ts Ex. 1 at 2. This Court reads *Greathouse* not as a bar to the search of Perez's room, but only as a possible bar to the search of Atterberry's or Ramos's room, which were never searched by officers executing this warrant. In addition, this issue was only stated as an alternate and not the primary basis for suppression.

Even if the defendant could prove that 7608 Scenic Brook Drive was a multiple-occupancy structure such that the warrant should have specified the particular subunit to be searched, the Court finds that this search falls within an exception to the specificity requirement. Where the building in question outwardly appears to be a single-occupancy structure and neither affiant nor the other investigating and executing officers knew or had reason to know of the structure's actual multiple-occupancy character until execution of the warrant was under way, the

---

[3] The Court notes that there was no such sign or indication not to enter on Perez's door, when the warrant was executed.

warrant is not defective for failure to specify a subunit within this named building. *United States v. Hinds*, 856 F.2d 438, 442 (1st Cir. 1988); *United States v. Maneti*, 781 F. Supp. 169, 179 (W.D.N.Y. 1991); *see also United States v. Davis*, 557 F.2d 1239, 1248 (8th Cir. 1977) (search warrant was held valid even though application stated a street address which turned out to include separate apartments, where officers had reason to believe it was a single family dwelling, and where, when officers conducting search discovered the separate occupancy of two apartments, they did not search those areas any further). Another case the Court finds persuasive is *United States v. Kyle*, in which a warrant authorizing the search of a residence was held to allow the search of a locked bedroom inside, despite Defendant's contention that the bedroom was a separate residence, where the room had neither its own access from outside, its own doorbell, nor its own mailbox. 40 F.3d 519, 524 (2d Cir. 1994).

Based on the officers' testimony and the photographs admitted as evidence at the hearing, the Court finds that the officers' conduct in executing the warrant was objectively reasonable under *Garrison*, and, alternatively, it falls under the exception stated above because 7608 Scenic Brook Drive outwardly appeared to be a single occupancy structure.

C. Reckless Disregard for Truth in Search Warrant Affidavit

Next, Defendant alleges that the search warrant affidavit contained a false statement made with reckless disregard for the truth because the evidence contained in it did not indicate that there were multiple people living at

7608 Scenic Brook Drive, Defendant argues that surveillance, trash inspection, and Department of Public Safety record inquiries would have revealed that Javier Perez was not the only resident of 7608 Scenic Brook Drive.

Where a warrant affidavit contains a false statement made intentionally, knowingly, or with reckless disregard for the truth, the good faith exception to the exclusionary rule does not apply. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978); *United States v. Cavazos*, 288 F.3d 706, 709-10 (5th Cir. 2002). The initial burden is on the defendant to prove by a preponderance of the evidence that false information was given intentionally or recklessly. *Cavazos*, 288 F.3d at 710. If the defendant cannot meet this burden, or if the affidavit would have sufficiently provided probable cause without the false information, the warrant did not violate the Fourth Amendment and the evidence is admissible. *Id.* In this case, Defendant contends that the false statement contained in the affidavit was the absence of any indication that Javier Perez lived with two other men at 7608 Scenic Brook Drive. Defendant asserts that Special Agent Britt recklessly disregarded the truth by not undertaking additional surveillance and inquiries which would have informed him that others were living with Javier Perez at the time he applied for the search warrant. However, these arguments fail.

Special Agent Britt never made a false statement of any kind in the affidavit; he based his testimony on accurate information that he had obtained from the Buffalo, NY Division of the FBI and he even confirmed that Perez resided at 7608 Scenic Brook Drive by doing utilities, credit, and internet searches before applying for the warrant. Britt testified that he did not know that anyone else was living at the residence until after arriving

to execute the warrant. Defendant has not proven by a preponderance of the evidence that any of the defendant's assertions in the affidavit were even untrue, let alone that Special Agent Britt recklessly disregarded the truth when making them. Assuming the affidavit contained an implicit representation that Javier Perez was the sole occupant of the residence, there was a substantial basis for such a conclusion at the time it was executed. Therefore, the Court finds no merit in the defendant's argument that the warrant should be invalidated for containing a false statement made with reckless disregard for the truth.

D. Description of Premises on Face of Search Warrant

Finally, Defendant complains that the search warrant omitted a description of the premises to be searched. Def's. Ex. 1. After closely examining the exhibit and its accompanying affidavit, the Court finds that the place to be searched was specifically indicated more than once. On the search warrant itself, although there is no description of the premises in the middle of the page following a checked box and "on the premises known as", one need only look a few lines above to the style of the case to see plainly stated "In the Matter of the Search of A residence, business, outbuildings, and motor vehicles on the curtilage located at: 7608 Scenic Brook Drive, Austin, Texas 78736." *Id.*

The Supreme Court has admonished that in construing search warrants there is no place for the "[t]echnical requirements of elaborate specificity once exacted under common law pleadings." *United States v. Ventresca*, 380 U.S. 102, 108 (1965). "It is enough if the description is

such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended." *Steele v. United States*, 267 U.S. 498, 503 (1925).

Here, the correct address of the place to be searched can be found both on the face of the search warrant and in the accompanying affidavit. Although the Court finds no ambiguity on the face of this warrant, even if there was, the Fifth Circuit allows this Court to consider the accompanying affidavit to clarify an ambiguity on the face of the warrant. *United States v. Haydel*, 649 F.2d 1152, 1157 (5th Cir. 1981). On page one of Britt's affidavit, the address "7608 Scenic Brook Drive, Austin, Texas 78736" is listed twice as the property to be searched. Gov'ts Ex. 11 at 2. Looking at both the face of the warrant and the accompanying affidavit, this Court finds no deficiency in the description of the place to be searched. The officers in this case indicated no difficulty in identifying 7608 Scenic Brook Drive as the place to be searched and they actually executed their search at exactly that address.

E. Good Faith Exception

Although this Court has based its opinion on the underlying search to this point, in the alternative, the Court holds that the good faith exception also militates in favor of denying Defendant's motion to suppress. In reviewing suppression motions, courts have the discretion to proceed directly to an analysis of the good-faith exception to the exclusionary rule announced in *United States v. Leon*, without first addressing the underlying Fourth Amendment question. 468 U.S. 897, 924-25 (1984). Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is

admissible nonetheless, so long as the executing officers' reliance on the warrant was objectively reasonable and in good faith. *Id.* at 921-25.

Both Agent Britt and Sergeant Eckert testified that they had no knowledge not reason to know that anyone else lived at 7608 Scenic Brook Drive besides the defendant until after they arrived to execute the warrant. When they discovered that others lived there, they refrained from searching the bedrooms of Atterberry and Ramos, even though their warrant authorized a search of the entire premises, and focused only on Javier Perez's bedroom and common areas. This restraint itself convinces the Court that the officers executed the warrant in good faith and in an objectively reasonable manner. Defendant does not address the good faith exception in his motion and does not raise any persuasive reason why it should not apply on these facts.

Therefore, even if the Defendant could prevail on any of his claims that the warrant was improperly executed, the good-faith exception would validate the government's search and preserve the items seized as admissible evidence.

III. Conclusion

Accordingly,

IT IS ORDERED Defendant Javier Perez's Motion to Suppress [#9] and Defendant's Supplemental Motion to Suppress [#14] are DENIED.

SIGNED this the 16th day of September 2005.

/s/ Sam Sparks
SAM SPARKS
UNITED STATES DISTRICT
JUDGE

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 06-50041

UNITED STATES OF AMERICA

Plaintiff-Appellee

v.

JAVIER PEREZ

Defendant-Appellant

Appeal from the United States District Court for the Western District of Texas, Austin

---

ON PETITION FOR REHEARING

(Filed May 29, 2007)

Before KING, GARZA, and PRADO, Circuit Judges.

PER CURIAM:

IT IS ORDERED that the petition for rehearing is DENIED.

ENTERED FOR THE COURT:

/s/ Edward C. Prado
United States Circuit Judge

United States District Court

Austin Division

In the Matter of the Search of (Name, address or brief description of person, property or premises to be searched)	APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT
A residence, business, outbuildings, and motor vehicles on the curtilage located at:	CASE NUMBER: A-04-181M
7608 Scenic Brook Drive Austin, TX 78736	(Filed Jun. 7, 2004)

I, Robert W. Britt, being duly sworn, depose and say:

I am a Special Agent with the Federal Bureau of Investigation and have reason to believe that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

in the Western District of Texas, there is now concealed a certain person or property, namely (describe the person or property)

See Attached Affidavit

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

concerning a violation of Titles 18, United States Code, Section(s) 2251 and 2252.

The facts to support a finding of probable cause are as follows:

See attached affidavit

Continued on the attached sheets and made a part hereof:
☒ Yes ☐ No

/s/ Robert Britt
Signature of Law Enforcement Agent

Sworn to before me and subscribed in my presence,

June 7, 2004
Date

Austin, Texas
City and State

ROBERT PITMAN
U.S. MAGISTRATE JUDGE
Name & Title of Judicial Officer

/s/ Robert Pitman
Signature of Judicial Officer

STATE OF TEXAS §
§
COUNTY OF TRAVIS §

AFFIDAVIT

I, Robert W. Britt, Special Agent, Federal Bureau of Investigation, Austin, Texas being duly sworn, states as follows:

1. Your affiant is a Special Agent of the Federal Bureau of Investigation, and has been so employed for over three years. Your affiant is currently assigned to Squad 12 in the Austin Resident Agency of the San Antonio Division.

2. The statements contained in this affidavit are based on information provided to me by Special Agent Ann M. Miller, FBI Buffalo, Jamestown Resident Agency, and

through my personal knowledge gained by my participation in this investigation. For the purpose of supporting an application for a search warrant, your affiant has set forth herein the facts that he believes are necessary to establish probable cause to believe that evidence exists for violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, and is located at 7608 Scenic Brook Drive, Austin, Texas 78736.

3. The property to be searched is the residence of Javier Perez. Perez's residence is located at 7608 Scenic Brook Drive, Austin, Texas 78736. The items to be seized from Perez's residence, including all computer hardware, software, related computer devices, paper, binders are described herein and in Attachment A to this Affidavit.

A. Any and all computers (including file servers, desktop computers, laptop computers, mainframe computers, and storage devices such as hard drives, removable drives, Zip disks, compact disks, and floppy disks) that were or appear to be capable of being used as a means to provide images of child pornography over the Internet in violation of 18 USC § 2252A may be seized.

B. Any and all computers seized may be searched for any evidence of violations of 18 USC 2252A, such search to include, but not be limited to, a search for image files, video, zip files, email content, TimeWarner Roadrunner user identification, TimeWarner Roadrunner log in records, addresses, group addresses, groups, temporary internet folders, cache files, .html pages, address books, sent folders, inbox, deleted folders, trash folders, text, group/chat room dialogue, cookies, newsgroups, internet relay chat or chat rooms, instant messages, and deleted files.

C. Telecommunications devices or equipment that may contain evidence of violations of 18 USC § 2252A, or may have been used to violate 18 USC § 2252A

D. Photographic, video equipment, or other electronic media that may contain evidence of violations of 18 USC § 2252.A, or may have been used to violate 18 USC § 2252A.

E. Papers or documents that may be evidence of violations of 18 USC §2252A, such as papers that document ownership or use of a computer.

F. Magazines, books, pictures, videos, calendars, diaries, date books, or periodicals that may be evidence of violations of 18 USC §2252A.

G. Any electronic media containing software which can be used to remove digital evidence from electronic media that may be evidence of violations of 18 USC §2252A.

H. Any document, record, or item that may be evidence of the location of any occupant of 7608 Scenic Brook Drive, Austin, Texas 78736 for the period February 27, 2003 to date.

I. Any document, item, or record that may bear a relationship to the Time Warner Roadrunner login "stephanmee2003."

J. Child Pornography, as defined in Title 18, United States Code, Section 2256.

4. As set forth in more detail below, there is probable cause to believe that Perez has committed violations of Title 18, United States Code, Sections 2251, 2252 and

2252A. The facts set forth in this affidavit are based on communications with FBI Special Agent Ann M. Miller.

5. It has been Affiant's experience that persons interested in child pornography keep and store material documenting the arrangements, the introduction, and tasks to consummate the acquisition of child pornography. The storage of such material can be for months and even years, and such persons are sometimes not even aware the storage occurs, due to the fact even "deleted" items can be recovered from the hard drive. Indeed, since the mid 1990s the computer has become the ideal mechanism for storing such material, insofar as a computer can hold hundreds or thousands of images and text documents in a compact space hidden from sight, protected from the eyes of others, but nonetheless easily retrievable by the user.

6. From his experience and training, Affiant knows that persons involved in viewing, sending or receiving child pornography tend to retain said material for extended periods, months or even years. The visual images obtained, traded, and/or sold are prized by those individuals interested in child pornography. In addition to their emotional value to the collector (usually quite significant in Affiant's experience), the visual images are intrinsically valuable for trading or selling and therefore are destroyed or deleted only rarely by the collector.

> (a) Special Agent Kenneth Lanning of the FBI, a widely acknowledged expert in the field of on-line child exploitation, has aptly noted that collectors swap pornographic photographs the way boys swap baseball cards. @ K. LANNING, CHILD MOLESTERS: A BEHAVIORAL ANALYSIS 28 (National Center for Missing and Exploited Children, 3d. ed. 1992).[1] Agent Lanning has found that no

> matter how much child pornography the collector has, he never has enough; and he rarely throws anything away.@ (*id.* at 29). Even if evidence of the existence of a child pornography collection is several years old, Agent Lanning believes that chances are he still has the collection now only it is larger.@ (*See id.*).

7. Collectors of child pornography have told Affiant personally in debriefings that the most efficacious way to expand a collection of child pornography is to offer another collector (via a trade over the Internet) images that the trading partner does not already possess. Accordingly, it is necessary to keep a great number of images in storage so as to have adequate material to allow participation in this informal barter system. The tendency to store child pornography is enhanced by the increased sense of security that a computer affords through its compact size and the ability with a computer, via passwords and otherwise, to keep others from looking at their material.

8. From his experience and training, Affiant knows that persons who use personal computers in their homes tend to retain their personal files and data for extended periods; months or even years. Affiant knows that due to a personal computer's unique ability to store large amounts of data for extended periods without consuming much, if any, additional physical space; people tend to retain this data. Affiant knows this to be true regardless of whether or not a person has traded-in or "upgraded" to a new personal computer. Affiant knows personal computer users to routinely transfer most of their data onto their new computers when making an upgrade. This data transfer is often done by saving files from the old computer to media sources (CDs or floppy disks, etc.) then opening onto the

new computer and saving them to the new hard drive. Visual images, such as child pornography, are as likely (if not more so) as other data to be transferred to a person's new, replacement or upgraded computer system.

9. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

Summary of Relevant Computer and Internet Concepts

10. The Internet is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet frequently cross state and international borders, even if those computers are in the same state.

11. Computers connected to the Internet are identified by addresses. Internet addresses take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can identify a physical location of a computer connection.

12. Computers use User Identities (User ID) or accounts to identify specific computer users. Users of a computer are assigned a unique account/User ID that is protected from unauthorized access by a password.

13. Each person connected to the Internet utilizes a unique Internet Protocol address ("IP address") – likened to a telephone number that can be used to identify a user's computer. With an IP address and an exact time, a suspect's computer can be tracked down by contacting the Internet Service Provider.

14. This investigation involves the use of web cam technology. Web cam technology has made it possible to send and receive video images throughout the Internet. The new innovations combined with high-speed Internet access have contributed rapid growth in the use of web cam technology. The process involves video streaming – a flow of still digital pictures snapped by a simple camera. The camera can be digital or analog. Analog cameras are like the traditional 8mm and VHS camcorders and are connected to a video card on a computer. That computer can upload the video stream to the Internet if connected via phone modem or direct connection. Digital webcams are a recent innovation facilitating "webcasting" from their own embedded webserver and webpage with a direct connection to the Internet. When the camera sends its stream of images to a server, the server holds a cache of images that are constantly updated. The webpage that webcasts the images contains an html code that identifies the source of the image, quality settings and size of the image to be displayed on the page. When a user's browser logs on, the stream of images are displayed within the window. The refresh rate determines the lag time between new images being displayed. This can range from one refresh every 90 seconds, for example, to near video quality streaming. This capability is determined by the speed of the connection (known as bandwith), the processing speed of all computers involved, the version of the

network browser, the chosen picture size, detail of the image, and network traffic. Any computer with a speed of 300mHz and above can display streaming video. Image quality is controlled through the level of compression; where high compression produces small files while low compression displays high image quality and larger files.

SUMMARY OF INVESTIGATION

15. I am familiar with the following facts based upon information officially supplied to me by FBI Special Agent Ann M. Miller, FBI Buffalo Division.

16. On March 3, 2004, Officer Carl Caprino, Lakewood-Busti Police Department, Lakewood, New York, contacted the FBI Buffalo Division, Jamestown Resident Agency regarding a child pornography complaint he had taken on February 27, 2004. Officer Caprino explained he was dispatched to 3017 Garfield Road, Lot2E, Jamestown, New York, to interview complainant Amanda Decker. During the interview, Decker was on line with an individual showing her child pornography via a webcam. Officer Caprino observed two females about ten years old running around a bedroom. One girl was completely naked and the other girl had only a skirt on with no underwear. Decker had been communicating with the individual via the computer since approximately 5:42 that afternoon and the individual had shown Decker several videos of child pornography.

17. On March 4, 2004, SA Ann M. Miller interviewed Decker at her residence. Decker explained that on February 26, 2004 she was in a bisexual chat room on Yahoo. On February 27, 2004 Decker received an instant message through Yahoo instant messaging from the Yahoo ID

"famcple." "Famcple" said he saw Decker in the chat room the day before. A short time later "Famcple" showed Decker two girls approximately 13 to 15 years old engaged in sexual acts with each other. Decker said these two girls were lying on a bed in front of the webcam. Decker thought this could have been live via the webcam. Decker said famcple then showed her a video of a four-year-old female engaged in sexual acts with an adult female. Decker was then shown a video of an eight-year-old male engaged in sexual acts with a six or seven year old girl. The next clip was the same six or seven-year-old girl engaged in sexual acts with an adult male. Decker believed "famcple" was playing these videos on his television and then showing them to her via the webcam. "Famcple" told Decker he received the videos from a "guy" who sent them to him. "Famcple" also told Decker that he sent the same guy some videos back. Finally, "famcple" showed Decker a video of two eight to ten year old females in ballet dresses. Decker said neither one of them had shirts on and they did not have anything on underneath their ballet dresses. Decker said this is the video Officer Caprino saw.

18. On March 5, 2004 an Administrative Subpoena was sent to Yahoo! Incorporated, Attn: Kathy McGoff, 701 First Avenue, Sunnyvale, CA, 408-349-5497, for any and all subscriber, account, and IP history information for the user of Yahoo ID, "famcple."

19. March 18, 2004, Yahoo! in response to the above subpoena, provided the following information:

Login Name:	stephanmee2003
Yahoo Mail Name:	*stephanmee2003@yahoo.com*
(Alternate) Email:	*dinog@exite.com*

Registration IP Address:	24.27.53.230
Other Identities:	stephanmee2003
	dinog79
	famcple
	stephdi2004
	famcp222
Full Name:	Mr. Rob Ram
City:	Beverly Hills
State:	CA.
Country:	United States
Zip:	90210
Account Created:	Sun Jan 4 15:52:00 2004
My Yahoo Configured:	Sun Jan 4 16:01:58 2004

Yahoo! also provided IP address information for the above account between February 18, 2004 and March 8, 2004. The account information in association with this case is as follows:

Login	IP Address	Day	Date	Local Time (EST)
Stephanmee2003	24.27.21.6	Thu	2004-02-26	17:50:58
Stephanmee2003	24.27.21.6	Thu	2004-02-26	17:51:02
Stephanmee2003	24.27.21.6	Thu	2004-02-26	18:42:02
Stephanmee2003	24.27.21.6	Thu	2004-02-27	18:35:48
Stephanmee2003	24.27.21.6	Thu	2004-02-27	18:35:49
Stephanmee2003	24.27.21.6	Thu	2004-02-27	19:15:35

20. On April 29, 2004, SA Miller spoke with Darcie Riedel of Yahoo! Incorporated regarding the account of stephanmee2003. Riedell confirmed stephanmee2003 is the login ID and is what would show up in their records even if the associated screen name "famcple" is used during a login session.

21. Special Agent Kenneth Jensen, FBI Buffalo, using the Internet search tool www.geektools.com, identified Time Warner Cable as the owner of the IP address **24.27.21.6**.

22. On March 19, 2004, Time Warner Cable, 290 Harbor Drive, Stamford, CT, 203-328-0645, was served with an Administrative Subpoena in regards to any and all subscriber, account, billing and service type information for the user of IP address 24.27.21.6 as used on 2/27/2004 between the hours of 1835 and 1915 (EST).

23. On March 24, 2004 Time Warner Cable provided the following information regarding the Road Runner Account assigned the above IP Address:

Name:	Javier Perez
Address:	7608 Scenic Brook Drive,
	Austin, Texas 788736
Phone:	512-288-4379
Usernames:	jperez

24. A public records check through Choicepoint identified Javier Perez with a social security number of 455-35-9931. The associated address and phone number listed was 7608 Scenic Brook Drive, Austin, Texas and 512-288-4379.

25. A white pages check via the Internet revealed phone number 512-288-4379 was associated with Javier Perez of 7608 Scenic Brook Drive, Austin, Texas 78736.

Instrumentalities and Evidence of the Crime

25. Based upon the facts contained in this Affidavit and Application, there is probable cause believe that a computer(s) located at 7608 Scenic Brook Drive, Austin, Texas 78736, has been used to commit the offense of possession, transmission, and trafficking of child pornography.

Items to be seized

The items your affiant seeks to seize are those evidencing violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, including but not limited to the following:

A. Any and all computers (including file servers, desktop computers, laptop computers, mainframe computers, and storage devices such as hard drives, removable drives, Zip disks, compact disks, and floppy disks) that were or appear to be capable of being used as a means to provide images of child pornography over the Internet in violation of 18 USC § 2252A may be seized.

B. Any and all computers seized may be searched for any evidence of violations of 18 USC 2252A, such search to include, but not be limited to, a search for image files, video, zip files, email content, TimeWarner Roadrunner user identification, TimeWarner Roadrunner log in records, addresses, group addresses, groups, temporary internet folders, cache files, .html pages, address books, sent folders, inbox, deleted folders, trash folders, text,

group/chat room dialogue, cookies, newsgroups, internet relay chat or chat rooms, instant messages, and deleted files.

C. Telecommunications devices or equipment that may contain evidence of violations of 18 USC § 2252A, or may have been used to violate 18 USC § 2252A

D. Photographic, video equipment, or other electronic media that may contain evidence of violations of 18 USC § 2252A, or may have been used to violate 18 USC § 2252A.

E. Papers or documents that may be evidence of violations of 18 USC §2252A, such as papers that document ownership or use of a computer.

F. Magazines, books, pictures, videos, calendars, diaries, date books, or periodicals that may be evidence of violations of 18 USC §2252A.

G. Any electronic media containing software which can be used to remove digital evidence from electronic media that may be evidence of violations of 18 USC §2252A.

H. Any document, record, or item that may be evidence of the location of any occupant of 7608 Scenic Brook Drive, Austin, Texas 78736 for the period February 27, 2003 to date.

I. Any document, item, or record that may bear a relationship to the Time Warner Roadrunner login "stephanmee2003."

J. Child Pornography, as defined in Title 18, United States Code, Section 2256.

Conclusion

Based on the information outlined above, there is probable cause to believe that located at 7608 Scenic Brook Drive, Austin, Texas 78736 there currently exist evidence of violations of Title 18, United States Code, Sections 2251, 2252 and 2252

/s/ Robert Britt
SPECIAL AGENT
ROBERT W. BRITT
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence this 7th day of June, 2004.

/s/ Robert Pitman
UNITED STATES
MAGISTRATE JUDGE
WESTERN DISTRICT OF TEXAS

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA	) Docket No. A 05-CR-155(1) SS
vs.	) Austin, Texas
JAVIER PEREZ	) September 15, 2005

TRANSCRIPT OF MOTION TO SUPPRESS
BEFORE THE HONORABLE SAM SPARKS

APPEARANCES:

For the United States:	Mr. Grant Sparks Assistant U.S. Attorney 816 Congress Avenue, Suite 1000 Austin, Texas 78701
For the Defendant:	Mr. Joshua D. Saegert Mr. Joseph A. Turner 1504 West Avenue Austin, Texas 78701
Court Reporter:	Ms. Lily Iva Reznik, RPR, CRR 200 W. 8th Street Austin, Texas 78701 (512) 916-5564

Proceedings recorded by mechanical stenography, transcript produced by computer.

* * *

[76] MR. SPARKS: Nothing further from the government, your Honor.

THE COURT: At the time that you executed the affidavit in front of Judge Pitman, you had this information that you have placed into evidence today; that

is, you've been furnished by the FBI agency in Buffalo with the information that the computer involved was related to the address, as I understand it, of 7608 Scenic Brook Drive, with the paid account of J. Perez, and you confirmed through the utilities that Javier Perez was allegedly the owner and in charge of the utilities of the house?

THE WITNESS: Yes, Your Honor.

THE COURT: Now, at that time, did you know or have any reason to believe yourself that there were other occupants renting any bedroom in that house?

THE WITNESS: No, Your Honor.

THE COURT: All right, Any further questions of this witness?

MR. SPARKS: None, your Honor.

MR. SAEGERT: None, your Honor.

THE COURT: You may step down.

MR. SPARKS: Government rests, your Honor.

THE COURT: All right. Have any further evidence?

MR. SAEGERT: No further evidence, your Honor.

THE COURT: Mr. Saegert, you have the lectern.

MR. SAEGERT: Judge, if I may. Four arguments today a [77] to why we're asking you to suppress any evidence obtained at 7608 Scenic Brook

Drive or obtained illegally, in violation of the Fourth and Fifth Amendments of the United States Constitution.

Under *Frank vs. Delaware*, evidence should be suppressed if the government has a reckless disregard for the truth of the information presented in the search warrant affidavit. And we're not arguing that the evidence that was presented to Judge Pitman was not truthful, but was not a complete truth. The government was reckless about what they provided to Judge Pitman when he was making his determination as to whether or not there was probable cause to search 7608 Scenic Brook –

THE COURT: Reckless in what sense? The FBI agent received the information from Buffalo as to the residential address. He confirmed that that information appeared to be correct from the utilities check. Where is there any recklessness? You indicated that you think that they should have been more observant and go out and have surveillance and a trash run, and that type of thing, to see whether or not there were renters in a residential home?

MR. SAEGERT: I think it was readily apparent that address that it was a multiple-person residence; there was not just one person living there. They could have driven by one time and probably determined that. In other words, they could have done a check through DPS as to who lived at that address, and the [78] reason that's important is because in the search warrant affidavit, the original return by Yahoo as to who that "famcple" user name was registered to was a "Rob Ram." A search of the internet would have shown that a Roberto – drawing a blank here.

THE COURT: Ramos.

MR. SAEGERT: Ramos was living there, a short version of Rob Ram. It would have been a glaringly obvious – or at least given Judge Pitman pause to think who else is living here, do you have the right person, because the only time Javier Perez' name ever came up was once – was through that Time Warner account. That's pretty common for one person to pay utilities for multiple people. Ask any college student on west campus.

THE COURT: A student on west campus in this residential area?

MR. SAEGERT: I pay utilities for me and my wife. We're two different people, granted that's one residence.

THE COURT: And they don't send you two bills, do they?

MR. SAEGERT; No, sir. They send me one bill, but I'm not charged for three separate IP addresses either. That was the other part of the reckless disregard for the truth. They sent a subpoena to Yahoo, asking for a lot of information, any subscriber account information. Yahoo sent back four lines – of Time Warner sent back four lines: Javier Perez, address, phone number, J. Perez. None of that matched up with "Stephanmee2003, who was the contact information through Yahoo, "famcple" or Rob [79] Ram, different names, no connection other than him having that account.

The information was – they were reckless in their disregard for that easily obtainable information. And it was readily apparent that there was not a single residence –

THE COURT: You know, I have two web addresses in my home. My wife and I have separate ones.

We have six children, thank God, are all gone, but I rather suspect that they would have separate addresses.

Well, let me extend the argument one more area. Give me your best shot. Assuming all of this to be true and assuming that the FBI should have – even on a pornography case when they've got no evidence of any indication where they've got any violence, unlike the drug cases, and let's just assume that they should have gone out and checked the trash, they should have gone out and asked the neighbors, they should have contacted the Department of Public Safety, all of that. How do you get past the good faith exception to the service of this –

MR. SAEGERT: I could answer that.

THE COURT: – Or this search where the FBI agent receives the information, it's all accurate, he puts it down, he gets a valid search warrant, purportedly, and he goes out and he finds Mr. Perez and he finds exactly what they're looking for.

MR. SAEGERT: Judge, to get around the good faith exception, their argument in good faith that they didn't know [80] anyone else, that's the government's position. Good faith, we thought that Javier Perez –

THE COURT: They're not arguing it, that's the evidence. You want that evidence to be there and it's there.

MR. SAEGERT: As soon as they came in the door and discovered Edwin Atterberry saying, I rent a room here, Roberto Ramos rents a room here, that good faith exception no longer exists. That evidence becomes stale because it's not the same evidence they were operating on when they presented that to Judge Pitman.

THE COURT: All right. I'll overrule the motion to suppress. I would not suppress this motion if they had searched the entire house under what they had, but they didn't search the entire house, for whatever reason it was. Maybe they are better constitutional scholars than the Court. But in any event, they searched Mr. – when they got in to see Mr. Ramos, he had the contraband there. They had a valid search warrant. I don't ever think you reach the good faith exception, but I will find it alternatively.

I find the affidavit was correct and contained accurate information. The information that was obtained from Buffalo, New York, FBI office, was confirmed by Agent Britt, placed in an affidavit. The search warrant was validly executed and validly submitted by Judge Pitman. And I will have a written opinion to you hopefully by noon tomorrow.

---

http://www.cybercrime.gov/s&smanual2002.htm.
Last visited on 8/13/07.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice

July 2002

TABLE OF CONTENTS

- PREFACE
- INTRODUCTION
- I. SEARCHING AND SEIZING COMPUTERS WITHOUT A WARRANT
  - A. Introduction
  - B. The Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers
    - 1. General Principles
    - 2. Reasonable Expectation of Privacy in Computers as Storage Devices
    - 3. Reasonable Expectation of Privacy and Third-Party Possession
    - 4. Private Searches
  - C. Exceptions to the Warrant Requirement in Cases Involving Computers
    - 1. Consent
      - a) Scope of Consent

- b) Third-Party Consent
- c) Implied Consent
- 2. Exigent Circumstances
- 3. Plain View
- 4. Search Incident to a Lawful Arrest
- 5. Inventory Searches
- 6. Border Searches
- 7. International Issues

- D. Special Case: Workplace Searches
  - 1. Private Sector Workplace Searches
    - a) Reasonable Expectation of Privacy in Private-Sector Workplaces
    - b) Consent in Private Sector-Work-places
    - c) Employer Searches in Private-Sector Workplaces
  - 2. Public-Sector Workplace Searches
    - a) Reasonable Expectation of Privacy in Public Workplaces
    - b) "Reasonable" Workplace Searches Under O'Connor v. Ortega
    - c) Consent in Public-Sector Workplaces

- II. SEARCHING AND SEIZING COMPUTERS WITH A WARRANT
  - A. Introduction
  - B. Planning the Search

- 1. Basic Strategies for Executing Computer Searches
  - a) When Hardware Is Itself Contraband, Evidence, or an Instrumentality or Fruit of Crime
  - b) When Hardware is Merely a Storage Device for Evidence of Crime
- 2. The Privacy Protection Act
  - a) A Brief History of the Privacy Protection Act
  - b) The Terms of the Privacy Protection Act
  - c) Application of the PPA to Computer Searches and Seizures
- 3. Civil Liability Under the Electronic Communications Privacy Act
- 4. Considering the Need for Multiple Warrants in Network Searches
- 5. No-Knock Warrants
- 6. Sneak-and-Peek Warrants
- 7. Privileged Documents
  - a) The Attorney General's Regulations Relating to Searches of Disinterested Lawyers, Physicians, and Clergymen
  - b) Strategies for Reviewing Privileged Computer Files

- C. Drafting the Warrant and Affidavit
  - Step 1: Accurately and Particularly Describe the Property to be Seized in the Warrant and/or Attachments to the Warrant
  - Step 2: Establish Probable Cause in the Affidavit

* * *

Step 2: Establish Probable Cause in the Affidavit

* * *

Probable cause challenges may also arise when supporting evidence in an affidavit derives heavily from records of a particular Internet account or Internet Protocol ("IP") address. The problem is a practical one: generally speaking, the fact that an account or address was used does not establish conclusively the identity or location of the particular person who used it. As a result, an affidavit based heavily on account or IP address logs must demonstrate a sufficient connection between the logs and the location to be searched to establish "a fair probability that contraband or evidence of a crime will be found in [the] particular place" to be searched. Gates, 462 U.S. at 238. See, e.g., United States v. Cervini, 2001 WL 863559 (10th Cir. Jul. 31, 2001) (unpublished) (upholding finding of probable cause to search a house based on evidence that a particular IP address was used to transmit child pornography at a particular time, that the IP address and time of transmission were associated with the suspect's account with an Internet service provider, and that the suspect had two active phone lines connected to the his house); United States v. Hay, 231 F.3d 630, 634 (9th Cir. 2000) (evidence that child pornography images were sent to an IP address associated with the defendant's apartment,

combined with other evidence of the defendant's interest in young children, created probable cause to search the defendant's apartment for child pornography); United States v. Grant, 218 F.3d 72, 76 (1st Cir. 2000) (evidence that an Internet account belonging to the defendant was involved in criminal activity on several occasions, and that the defendant's car was parked at his residence during at least one such occasion, created probable cause to search the defendant's residence).

* * *